Automorphism group of Cartan modular curves

Pietro Mercuri
a joint work with V. Dose and G. Lido

Sapienza Università di Roma

Modular curves and Galois representations
Zagreb, 18-09-2023

Modular curves as moduli spaces

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing $-I$, we associate a modular curve to H.

On the set of pairs (E, ϕ), where E is an elliptic curve and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$ is an isomorphism, we define the following equivalence relation:

$$(E, \phi) \sim_H (E', \phi') \iff \begin{array}{c}\text{there is an isomorphism } \iota\colon E \xrightarrow{\sim} E', \\ \text{and } (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi \in H.\end{array}$$

The modular curve Y_H is the coarse moduli space parametrizing $\{(E, \phi)\}/\sim_H$ and X_H is the compactification of Y_H. In particular, for every algebraically closed field K, there is a bijection between $Y_H(K)$ and $\{(E, \phi)\}/\sim_H$, where E is an elliptic curve over K.

Modular curves as moduli spaces

If $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then Y_H and X_H are geometrically connected algebraic curves defined over $\mathbb{Q}$. Moreover, there are isomorphisms of Riemann surfaces

$$Y_H(\mathbb{C}) \cong \Gamma_H \backslash \mathcal{H} \qquad \text{and} \qquad X_H(\mathbb{C}) \cong \Gamma_H \backslash \mathcal{H}^*,$$

where $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ is the complex upper half-plane, $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ is the extended complex upper half-plane,

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{n} \in H\},$$

is a congruence subgroup of level n and the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}^*$ is given, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}^*$, by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau := \frac{a\tau + b}{c\tau + d}.$$

Example: When $H = B(n) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}$ (the standard Borel subgroup), we have $X_H = X_0(n)$.

Rational points

One interesting problem is to determine the set of K-rational points of X_H for a number field K.

If the genus is at least 2, we know by Faltings Theorem that the number of K-rational points is finite. But we want to know precisely what they are.

This is hard even when $K = \mathbb{Q}$ and it is still an open problem although many improvements have been done.

Serre made a conjecture that describes the set of $\mathbb{Q}$-rational points $X_H(\mathbb{Q})$ when the level $n = p$ is prime.

Since the natural maps $X_{H_1} \to X_{H_2}$, induced by the inclusions $H_1 \subset H_2$, are rationals, it is enough to study X_H when H is a proper maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Toward maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

Let p be an odd prime and let ξ be a nonsquare modulo p, we define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$:

- the (standard) *split Cartan* subgroup

$$C_s(p) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p\mathbb{Z})^\times \right\};$$

- the normalizer of the (standard) split Cartan subroup

$$C_s^+(p) := C_s(p) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p\mathbb{Z})^\times \right\};$$

- the (standard) *nonsplit Cartan* subgroup

$$C_{ns}(p) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p\mathbb{Z}, (a, b) \not\equiv (0,0) \bmod p \right\};$$

- the normalizer of the (standard) nonsplit Cartan subroup

$$C_{ns}^+(p) := C_{ns}(p) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p\mathbb{Z}, (a, b) \not\equiv (0,0) \bmod p \right\}.$$

Cartan modular curves for prime levels

Correspondently we define the following modular curves:

$$X_s(p) := X_{C_s(p)}; \qquad X_{ns}(p) := X_{C_{ns}(p)};$$
$$X_s^+(p) := X_{C_s^+(p)}; \qquad X_{ns}^+(p) := X_{C_{ns}^+(p)}.$$

All of these are geometrically connected algebraic curves defined over $\mathbb{Q}$.

Moreover, if we define the following congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_s(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_s(p)\};$$
$$\Gamma_s^+(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_s^+(p)\};$$
$$\Gamma_{ns}(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_{ns}(p)\};$$
$$\Gamma_{ns}^+(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_{ns}^+(p)\}.$$

We have the following isomorphisms of Riemann surfaces:

$$X_s(p)(\mathbb{C}) \cong \Gamma_s(p)\backslash\mathcal{H}^*; \qquad X_{ns}(p)(\mathbb{C}) \cong \Gamma_{ns}(p)\backslash\mathcal{H}^*;$$
$$X_s^+(p)(\mathbb{C}) \cong \Gamma_s^+(p)\backslash\mathcal{H}^*; \qquad X_{ns}^+(p)(\mathbb{C}) \cong \Gamma_{ns}^+(p)\backslash\mathcal{H}^*.$$

Maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

If H_1 and H_2 are conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then $X_{H_1} \cong X_{H_2}$.

Theorem

Let p be an odd prime and let H be a proper maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/p\mathbb{Z})^\times$. Then, we can only have one of the following cases:

- *H is a Borel subgroup, i.e., it is a conjugate of $B(p)$;*
- *H is the normalizer of a split Cartan subgroup, i.e., it is a conjugate of $C_{\mathrm{s}}^+(p)$;*
- *H is the normalizer of a nonsplit Cartan subgroup, i.e., it is a conjugate of $C_{\mathrm{ns}}^+(p)$;*
- *H is an exceptional subgroup, i.e., its image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic either to the symmetric group S_4 or to the alternating group A_4 or A_5.*

Some rational points arise naturally, we call these points *expected rational points*.

Uniformity conjecture

Conjecture (Uniformity conjecture, Serre, 1972)

Let H_p be a maximal subgroup as above of the same type for every prime p. Then, there is a positive constant C such that the rational points of X_{H_p} are only the expected rational points for every $p > C$.

What is known?

- For the exceptional subgroups, this is true for $C = 13$.[a]
- For the Borel case, this is true for $C = 37$.[b]
- For the normalizer of a split Cartan subgroup, this is true for $C = 13$.[c]
- For the normalizer of a nonsplit Cartan subgroup, is this true?

In some cases the knowledge of automorphism group helped to study the rational points.[d,e]

[a] Serre, 1977
[b] Mazur, 1977
[c] Bilu, Parent, Rebolledo, 2013
[d] Kenku, 1981
[e] Momose, 1984

Automorphisms

Let $\mathrm{GL}_2^+(\mathbb{Q}) := \{g \in \mathrm{GL}_2(\mathbb{Q}) : \det g > 0\}$ and let

$$\pi\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q}) := \mathrm{GL}_2^+(\mathbb{Q})/\{\text{scalar matrices}\}$$

be the natural quotient map.

Each matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ defines a fractional linear transformation $m\colon \mathcal{H}^* \to \mathcal{H}^*$ and such an automorphism of the Riemann surface $\mathcal{H}^*$ pushes down to an automorphism of $\Gamma_H \backslash \mathcal{H}^*$ if and only if m normalizes $\pi(\Gamma_H)$.

Definition (Modular automorphisms)

If $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, an automorphism of X_H, defined over $\mathbb{C}$, is called *modular* if its action on $X_H(\mathbb{C}) = \Gamma_H \backslash \mathcal{H}^*$ is described by a fractional linear transformation of $\mathcal{H}^*$ associated to an element $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ that normalizes $\pi(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$.

Automorphisms

Is every automorphism of X_H modular?

The answer is no when the genus is 0 or 1. It is not hard to see that in these cases there are non-modular automorphisms.

It is true for $X_0(n)$ when the genus is at least 2 and $n \neq 37, 63, 108$.[f,g,h,i]

---

[f] Ogg, 1977
[g] Kenku, Momose, 1988
[h] Elkies, 1990
[i] Harrison, 2011

Cartan groups for prime power levels

We can extend the previous Cartan groups to prime powers:

$$C_s(p^r) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^r\mathbb{Z})^\times \right\};$$

$$C_s^+(p^r) := C_s(p^r) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^r\mathbb{Z})^\times \right\};$$

$$C_{ns}(2^r) := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, a, b \in \mathbb{Z}/2^r\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{ns}^+(2^r) := C_{ns}(2^r) \cup \left\{ \begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}/2^r\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

and for p odd and a nonsquare element $\xi \in (\mathbb{Z}/p^r\mathbb{Z})^\times$:

$$C_{ns}(p^r) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^r\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\};$$

$$C_{ns}^+(p^r) := C_{ns}(p^r) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^r\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}.$$

Cartan modular curves for prime power levels

Correspondently we define the following modular curves:

$$X_{\mathrm{s}}(p^r) := X_{C_{\mathrm{s}}(p^r)}; \qquad X_{\mathrm{ns}}(p^r) := X_{C_{\mathrm{ns}}(p^r)};$$
$$X_{\mathrm{s}}^{+}(p^r) := X_{C_{\mathrm{s}}^{+}(p^r)}; \qquad X_{\mathrm{ns}}^{+}(p^r) := X_{C_{\mathrm{ns}}^{+}(p^r)}.$$

All of these are geometrically connected algebraic curves defined over $\mathbb{Q}$.
If we define the following congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_{\mathrm{s}}(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{s}}(p^r)\};$$
$$\Gamma_{\mathrm{s}}^{+}(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{s}}^{+}(p^r)\};$$
$$\Gamma_{\mathrm{ns}}(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{ns}}(p^r)\};$$
$$\Gamma_{\mathrm{ns}}^{+}(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{ns}}^{+}(p^r)\}.$$

We have the following isomorphisms of Riemann surfaces:

$$X_{\mathrm{s}}(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{s}}(p^r)\backslash\mathcal{H}^*; \qquad X_{\mathrm{ns}}(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{ns}}(p^r)\backslash\mathcal{H}^*;$$
$$X_{\mathrm{s}}^{+}(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{s}}^{+}(p^r)\backslash\mathcal{H}^*; \qquad X_{\mathrm{ns}}^{+}(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{ns}}^{+}(p^r)\backslash\mathcal{H}^*.$$

Automorphisms of Cartan modular curves

Theorem (Dose, Lido, M., 2022)

If $p^r \notin \{2^3, 2^4, 2^5, 2^6, 3^2, 3^3, 11\}$, *then all the automorphisms of the curves* $X_s(p^r), X_s^+(p^r), X_{ns}(p^r), X_{ns}^+(p^r)$ *with genus at least 2 are modular and*

$$\mathrm{Aut}(X_s(p^r)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases}$$

$$\mathrm{Aut}(X_s^+(p^r)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3, \\ \{1\}, & \text{if } p > 3, \end{cases}$$

$$\mathrm{Aut}(X_{ns}(p^r)) \cong \mathbb{Z}/2\mathbb{Z},$$
$$\mathrm{Aut}(X_{ns}^+(p^r)) \cong \{1\},$$

with $(\varphi(1))(x, y) = (y, x)$ *and* S_3 *is the symmetric group acting on three elements.*

Automorphisms of modular curves of Cartan type

Let $n \in \mathbb{Z}_{\geq 3}$ with prime factorization $n = \prod_{i=1}^{\omega(n)} p_i^{e_i}$ and let $H \cong \prod_{i=1}^{\omega(n)} H_{p_i}$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, where H_{p_i} is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$.

Theorem (Dose, Lido, M., 2022)

If $n \geq 10^{400}$ and H such that, for each $i = 1, \ldots, \omega(n)$, either $H_{p_i} \in \{C_{\mathrm{s}}(p_i^{e_i}), C_{\mathrm{ns}}(p_i^{e_i})\}$ or $H_{p_i} \in \{C_{\mathrm{s}}^{+}(p_i^{e_i}), C_{\mathrm{ns}}^{+}(p_i^{e_i})\}$, then every automorphism of X_H is modular and we have

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H_2 = C_{\mathrm{s}}^{+}(2), \\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Outline of the proof: Step 1

Remind that $\pi\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q})$ is the natural quotient map and $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Remark that if $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of modular automorphisms is a subgroup of $\mathrm{Aut}(X_H)$ isomorphic to $N/\pi(\Gamma_H)$, where N is the normalizer of $\pi(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$.

Some computations with groups of matrices show that $N = \pi(\Gamma_{N'})$ (except in the special case $n \equiv 2 \bmod 4$).

Hence $N/\pi(\Gamma_H) = \pi(\Gamma_{N'})/\pi(\Gamma_H) = \pi(\Gamma_{N'})/\pi(\Gamma_{H'}) \cong N'/H'$.

Outline of the proof: Step 2

Prove that if there is a prime $\ell \nmid n$ such that $5 \le \ell \le \frac{1}{2}\mathrm{gon}(X_H) - 1$, where gon denotes the gonality, then each automorphism of X_H defined over a compositum of quadratic fields is modular.

In order to prove this we studied certain properties of Hecke operators not known before.

These properties are used to show that each automorphism of X_H defined over a compositum of quadratic fields preserves the set of cusps and the set of branch points.

And we are done since an automorphism is modular if and only if it preserves the set of cusps and the set of branch points[j].

The condition $\mathrm{gon}(X_H) > 2\ell + 1$ is used to move from the Jacobian to actual divisors showing that a principal divisor is in fact the zero divisor.

[j] Dose, 2016

Outline of the proof: Step 3

We can apply the previous step because by Abramovich's bound we have

$$\mathrm{gon}(X_H) \geq \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] \geq 10n.$$

Hence, for every $n > 1$ there is a prime $\ell \nmid n$ such that $5 \leq \ell < 5n - 1$.

Outline of the proof: Step 4

Prove that for $n \geq 10^{400}$, each automorphism is defined over a compositum of quadratic fields.

In order to prove this we used an extension of Chen's isogeny for passing from the modular curve of Cartan type (i.e., such that $H_{p_i} \in \{C_s(p_i^{e_i}), C_{ns}(p_i^{e_i})\}$ or $H_{p_i} \in \{C_s^+(p_i^{e_i}), C_{ns}^+(p_i^{e_i})\}$) to the curve $X_0(n)$.

Then we bounded the CM part of the Jacobian of $X_0(n)$ using some Grössencharacter theory from Shimura and bounding the cardinality of some class groups.

It is the bound for the class groups that gives the high lower bound for the level n in the statement. When n is a prime power this bound become easier and this allows to have better results as in the case of Cartan modular curves.

THANK YOU!